УДК 004.732.056

РАЗРАБОТКА МОДЕЛИ АНАЛИЗАТОРА ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ ВЕРОЯТНОСТНОГО АВТОМАТА

***В.В. ЧЕЛАК*[1*], *С.Ю. ГАВРИЛЕНКО*[2]**

[1] *магистрант кафедры ВТП, НТУ «ХПІ», Харьков, УКРАИНА*
[2] *проф. кафедры ВТП, канд. техн. наук, НТУ «ХПІ», Харьков, УКРАИНА*
[*] *email: victor.chelak@gmail.com*

Согласно полугодовому отчету Cisco по информационной безопасности в первой половине 2016 года отмечен рост количества и качества атак с применением программ-вымогателей, направленных как на отдельных пользователей, так и на организации. Успех недавних атак программ-вымогателей в отношении ряда компаний, включая медицинские учреждения, наверняка послужит заразительным примером для других хакеров [1]. Вирусы наносят убытки на десятки миллиардов долларов поэтому задача их оперативного выявления является актуальной [2, 3].

В докладе предложена модель анализатора вредоносного программного обеспечения на основе вероятностного автомата [4].

Вероятностный автомат (ВА) впервые был сформулировано в 1963 г. в основополагающей работе М. Рабина [5] и представляет собой синтез понятий конечного детерминированного автомата и цепи Маркова. Автомат предназначен для построения математических моделей динамических систем, в которых присутствует неопределённость, описываемая статистическими закономерностями. Эта неопределённость связана:

– с неточностью знаний о состояниях, в которых моделируемые системы находятся в процессе своего функционирования;

– с недетерминированностью правил изменения этих состояний.

Вероятностный автомат (рис. 1) функционирует путём выполнения переходов, после каждого из которых происходит обновление значений вероятностных переменных такого автомата в зависимости от реакции среды.

В общем случае ВА работает в некоторой среде, в которую он выдает выходные сигналы y_i и из которой он получает входные x_i.

Если автомат в момент времени t перешел из состояния s_m в состояние s_k и в момент времени $t+1$ получил сигнал «штраф», то вероятность p_{mk} заменяется на αp_{mk}, где коэффициент α больше 0 и меньше 1, а все остальные вероятности в строке изменяются на величину $(1-\alpha)p_{mk}/M$. Если же получил сигнал «нештраф», то вероятность p_{mk} увеличиться на величину $(1-\alpha)+\alpha p_{mk}$, а все

остальные уменьшаются на величину $(1-\alpha)(1-p_{mk})/M$, где M – количество внутренних состояний автомата.

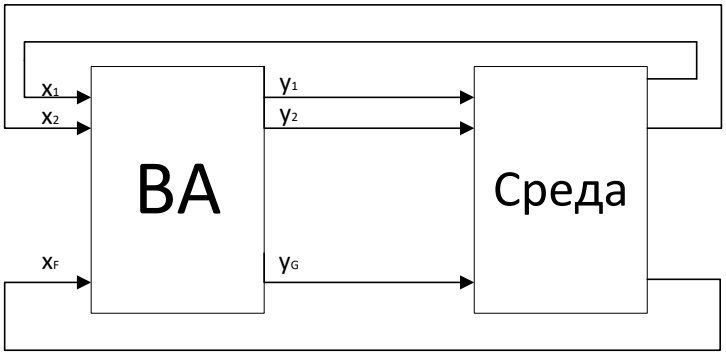

Рис. 1 – Схема работы вероятностного автомата

Принцип предложенной модели анализатора вредоносного программного обеспечения на основе вероятностного автомата заключается в проверке возможных сред обитания вирусов и выявлении в них команд (групп команд), характерных для вирусов. Каждая из подозрительных команд сопоставляется с множеством состояний s. Переход из состояния s_m в состояние s_k в момент времени t зависит от входного состояния и от значения маркера, представляющего собой вероятность перехода из состояния s_m в состояние s_k, зависящего от реакции среды.

Эвристические анализаторы при обнаружении "подозрительных" команд в файлах или загрузочных секторах выдают сообщение о возможном заражении. Введение дополнительных переходов и зацикленность на состояниях позволяют обнаружить модификацию известных вирусов.

Для идентификации состояния компьютерной системы в условиях вирусных атак была разработана программная модель на базе вероятностного автомата, позволяющая обнаружить вирусы типа «червь» и их модификации.

Полученные результаты подтвердили возможность использования предложенной модели на основе вероятностного автомата как дополнительного средства для выявления вирусных атак в общей системе обнаружения вредоносного программного обеспечения.

Список литературы:

1. Полугодовой отчет по ИБ от Cisco. [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru /blog/personal /Informacionnaya_ bezopasnost_v_detalyah/316275.php.

2. *Шелухин О.И.* Обнаружение вторжений в компьютерные сети / *О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова*. – М.: Гарячая линия-Телеком, 2013. – 220 с.

3. *Гошко С.В*. Технологии борьбы с компьютерными вирусами / *С.В. Гошко*. – М.: Солон-Пресс, 2009. – 352 с.

4. *Поспелов Д.А.* Вероятностные автоматы. – М.: Энергия, 1970. – 88 с.

5. *Rabin, M.O*. Probabilistic automata. Information and Control 6 (3), 230–245 (1963) (русский перевод: Рабин М.О. Вероятностные автоматы / Кибернетический сборник, Вып. 9. – М.: Иностранная литература, 1964. – С. 123-141.